

**IN THE CLAIMS:**

1           1.       (Original) An elliptic curve arithmetic operation device for performing one of an  
2       addition and a doubling on an elliptic curve  $E: y^2 = f(x)$  on a residue class ring of polynomials  
3       in two variables  $\alpha$  and  $\beta$ , moduli of the residue class ring being polynomials  $\beta^2 - f(\alpha)$  and  $h(\alpha)$ ,  
4       where  $f(\alpha) = \alpha^3 + a\alpha + b$ ,  $a$  and  $b$  are constants, and  $h(\alpha)$  is a polynomial in the variable  $\alpha$ , the  
5       elliptic curve arithmetic operation device comprising:

6                 acquiring means for acquiring affine coordinates of at least one point on the  
7       elliptic curve  $E$  and operation information indicating one of the addition and the doubling, from  
8       an external source;

9                 transforming means for performing a coordinate transformation on the acquired  
10      affine coordinates to generate Jacobian coordinates, the coordinate transformation being  
11      transforming affine coordinates  $(\phi(\alpha), \beta x \phi(\alpha))$  of a given point on the elliptic curve  $E$  using  
12      polynomials

$$X(\alpha) = f(\alpha) \times \phi(\alpha)$$

$$Y(\alpha) = f(\alpha) \times 2x\phi(\alpha)$$

$$Z(\alpha) = 1$$

16               into Jacobian coordinates  $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha))$ ,  $\phi(\alpha)$  and  $\varphi(\alpha)$  being  
17      polynomials; and

18               operating means for performing one of the addition and the doubling indicated by  
19      the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian  
20      coordinates of a point on the elliptic curve  $E$ .

2. (Original) The elliptic curve arithmetic operation device of Claim 1,

wherein the acquiring means

(a) in a first case acquires affine coordinates of two different points on the elliptic curve  $E$  and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve  $E$  and operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating means

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve  $E$ , and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve  $E$ .

3. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

wherein in the first case

the acquiring means acquires affine coordinates

$$(\cancel{X_1(\alpha)}, \cancel{\beta x Y_1(\alpha)}) (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

$$(\cancel{X2(\alpha)}, \cancel{\beta x Y2(\alpha)}) (\phi_2(\alpha), \beta x \phi_2(\alpha))$$

of the two different points on the elliptic curve  $E$  and the operation information indicating the addition,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$$

of the two different points, and

the operating means computes

$$U1(\alpha) = X1(\alpha) x Z2(\alpha) \{ 2$$

$$U2(\alpha) = X2(\alpha) x Z1(\alpha) \{ 2$$

$$S1(\alpha) = Y1(\alpha) x Z2(\alpha) \{ 3$$

$$S2(\alpha) = Y2(\alpha) x Z1(\alpha) \{ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha) \{ 3 - 2x U1(\alpha) x H(\alpha) \{ 2 + r(\alpha) \{ 2$$

$$Y3(\alpha) = -S1(\alpha) x H(\alpha) \{ 3 + r(\alpha) x (U1(\alpha) x H(\alpha) \{ 2 - X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha) x Z2(\alpha) x H(\alpha)$$

to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the elliptic curve  $E$ .

4. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

wherein in the second case

the acquiring means acquires affine coordinates

$$(\cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)}) (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

of the single point on the elliptic curve  $E$  and the operation information indicating

the doubling,

the transforming means performs the coordinate transformation on the acquired

affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

of the single point, and

the operating means computes

$$S(\alpha) = 4 x X1(\alpha) x Y1(\alpha) \{ 2$$

$$M(\alpha) = 3 x X1(\alpha) \{ 2 + a x Z1(\alpha) \{ 4 x f(\alpha) \{ 2$$

$$T(\alpha) = -2 x S(\alpha) + M(\alpha) \{ 2$$

and computes

$$X3(\alpha) = T(\alpha)$$

$$Y3(\alpha) = -8 x Y1(\alpha) \{ 4 + M(\alpha) x (S(\alpha) - T(\alpha))$$

$$Z3(\alpha) = 2 x Y1(\alpha) x Z1(\alpha)$$

to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the elliptic

curve  $E$ .

5. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,

wherein the acquiring means

(a) in the first case acquires affine coordinates

$$\langle \cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)} \rangle \langle \phi_1(\alpha), \beta x \phi_1(\alpha) \rangle$$

$$\langle \cancel{X2(\alpha)}, \cancel{\beta x Y2(\alpha)} \rangle \langle \phi_2(\alpha), \beta x \phi_2(\alpha) \rangle$$

of the two different points on the elliptic curve  $E$  and the operation information

indicating the addition, and

(b) in the second case acquires affine coordinates

$$\langle \cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)} \rangle \langle \phi_1(\alpha), \beta x \phi_1(\alpha) \rangle$$

of the single point on the elliptic curve  $E$  and the operation information indicating

the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired

affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired

affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

of the single point, and

wherein the operating means

(a) in the first case computes

$$U1(\alpha) = X1(\alpha) \times Z2(\alpha) \quad \{ 2$$

$$U2(\alpha) = X2(\alpha) \times Z1(\alpha) \quad \{ 2$$

$$S1(\alpha) = Y1(\alpha) \times Z2(\alpha) \quad \{ 3$$

$$S2(\alpha) = Y2(\alpha) \times Z1(\alpha) \quad \{ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha) \quad \{ 3 - 2 \times U1(\alpha) \times H(\alpha) \quad \{ 2 + r(\alpha) \quad \{ 2$$

$$Y3(\alpha) = -S1(\alpha) \times H(\alpha) \quad \{ 3 + r(\alpha) \times (U1(\alpha) \times H(\alpha) \quad \{ 2 - X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$  of the point on the elliptic curve  $E$ , and

(b) in the second case computes

$$S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha) \quad \{ 2$$

$$M(\alpha) = 3 \times X1(\alpha) \quad \{ 2 + a \times Z1(\alpha) \quad \{ 4 \times f(\alpha) \quad \{ 2$$

$$T(\alpha) = -2 \times S(\alpha) + M(\alpha) \quad \{ 2$$

and computes

$$X3(\alpha) = T(\alpha)$$

$$Y3(\alpha) = -8 \times Y1(\alpha) \quad \{ 4 + M(\alpha) \times (S(\alpha) - T(\alpha))$$

$$Z3(\alpha) = 2 \times Y1(\alpha) \times Z1(\alpha)$$

to obtain the Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$  of the point on the elliptic curve  $E$ .

6. (Original) An elliptic curve order computation device for computing an order of an elliptic curve according to a Schoof-Elkies-Atkin algorithm, comprising the elliptic curve arithmetic operation device of Claim 1.

7. (Original) The elliptic curve order computation device of Claim 6 comprising the elliptic curve arithmetic operation device of Claim 2.

8. (Original) The elliptic curve order computation device of Claim 7 comprising the elliptic curve arithmetic operation device of Claim 5.

9-22. (Cancelled)

23. (Currently Amended) An elliptic curve arithmetic operation method used in an elliptic curve arithmetic operation device equipped with an acquiring means, a transforming means, and an operating means, for performing one of an addition and a doubling on an elliptic curve  $E: y^2 = f(x)$  on a residue class ring of polynomials in two variables  $\alpha$  and  $\beta$ , moduli of the residue class ring being polynomials  $\beta^2 - f(\alpha)$  and  $h(\alpha)$ , where  $f(\alpha) = \alpha^3 + a\alpha + b$ ,  $a$  and  $b$  are constants, and  $h(\alpha)$  is a polynomial in the variable  $\alpha$ , the elliptic curve arithmetic operation method comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve  $E$  and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates,

13 the coordinate transformation being transforming affine coordinates  $(\phi(\alpha), \beta x \phi(\alpha))$  of a given  
14 point on the elliptic curve  $E$  using polynomials

$$15 \quad X(\alpha) = f(\alpha)x\phi(\alpha)$$

$$16 \quad Y(\alpha) = f(\alpha) \{ 2x\phi(\alpha)$$

$$17 \quad Z(\alpha) = 1$$

18 into Jacobian coordinates  $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha))$ ,  $\phi(\alpha)$  and  ~~$\phi(\alpha)$~~   $\underline{\phi(\alpha)}$  being  
19 polynomials; and

20 an operating step performed by the operating means, for performing one of the  
21 addition and the doubling indicated by the acquired operation information, on the generated  
22 Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve  $E$ .

1 24. (Cancelled)

1 25. (Original) A computer-readable storage medium storing an elliptic curve  
2 arithmetic operation program used in an elliptic curve arithmetic operation device equipped with  
3 acquiring means, transforming means, and operating means, for performing one of an addition  
4 and a doubling on an elliptic curve  $E: y^2 = f(x)$  on a residue class ring of polynomials in two  
5 variables  $\alpha$  and  $\beta$ , moduli of the residue class ring being polynomials  $\beta^2 - f(\alpha)$  and  $h(\alpha)$ , where  
6  $f(\alpha) = \alpha^3 + a\alpha + b$ ,  $a$  and  $b$  are constants, and  $h(\alpha)$  is a polynomial in the variable  $\alpha$ , the elliptic  
7 curve arithmetic operation program comprising:

8 an acquiring step performed by the acquiring means, for acquiring affine  
9 coordinates of at least one point on the elliptic curve  $E$  and operation information indicating one  
10 of the addition and the doubling, from an external source;



a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates  $(\phi(\alpha), \beta x \phi(\alpha))$  of a given point on the elliptic curve  $E$  using polynomials

$$X(\alpha) = f(\alpha)x\phi(\alpha)$$

$$Y(\alpha) = f(\alpha) \{ 2x\phi(\alpha)$$

$$Z(\alpha) = 1$$

into Jacobian coordinates  $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha))$ ,  $\phi(\alpha)$  and  $\varphi(\alpha)$  being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve  $E$ .

26. (Original) The storage medium of Claim 25, wherein the acquiring step

(a) in a first case acquires affine coordinates of two different points on the elliptic curve  $E$  and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve  $E$  and operation information indicating the doubling,

wherein the transforming step

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating step

(a) in the first case performs the addition indicated by the acquired operation

information on the generated Jacobian coordinates of the two different points to obtain the

Jacobian coordinates of the point on the elliptic curve  $E$ , and

(b) in the second case performs the doubling indicated by the acquired

operation information on the generated Jacobian coordinates of the single point to obtain the

Jacobian coordinates of the point on the elliptic curve  $E$ .

27. (Currently Amended) The storage medium of Claim 26, wherein in the first case the acquiring step acquires affine coordinates

$$(\cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)}) (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

$$(\cancel{X2(\alpha)}, \cancel{\beta x Y2(\alpha)}) (\phi_2(\alpha), \beta x \phi_2(\alpha))$$

of the two different points on the elliptic curve  $E$  and the operation information indicating the addition,

the transforming step performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$$

of the two different points, and

the operating step computes

$$U1(\alpha) = X1(\alpha)xZ2(\alpha) \{ 2$$

$$U2(\alpha) = X2(\alpha)xZ1(\alpha) \{ 2$$

$$S1(\alpha) = Y1(\alpha)xZ2(\alpha) \{ 3$$

$$S2(\alpha) = Y2(\alpha)xZ1(\alpha) \{ 3$$

$$17 \quad H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$18 \quad r(\alpha) = S2(\alpha) - S1(\alpha)$$

19 and computes

$$20 \quad X3(\alpha) = -H(\alpha) \{ 3 - 2xU1(\alpha)xH(\alpha) \{ 2 + r(\alpha) \{ 2$$

$$21 \quad Y3(\alpha) = -S1(\alpha)xH(\alpha) \{ 3 + r(\alpha)x(U1(\alpha)xH(\alpha) \{ 2 - X3(\alpha))$$

$$22 \quad Z3(\alpha) = Z1(\alpha)xZ2(\alpha)xH(\alpha)$$

23 to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the elliptic  
24 curve E.

1 28. (Currently Amended) The storage medium of Claim 26,

2 wherein in the second case the acquiring step acquires affine coordinates

$$3 \quad (\cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)}) \quad (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

4 of the single point on the elliptic curve E and the operation information indicating  
5 the doubling,

6 the transforming step performs the coordinate transformation on the acquired  
7 affine coordinates of the single point to generate Jacobian coordinates

$$8 \quad (X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

9 of the single point, and

10 the operating step computes

$$11 \quad S(\alpha) = 4xX1(\alpha)xY1(\alpha) \{ 2$$

$$12 \quad M(\alpha) = 3xX1(\alpha) \{ 2 + axZ1(\alpha) \{ 4xf(\alpha) \{ 2$$

$$13 \quad T(\alpha) = -2xS(\alpha) + M(\alpha) \{ 2$$

14 and computes

15 
$$X3(\alpha) = T(\alpha)$$

16 
$$Y3(\alpha) = -8xY1(\alpha) \{ 4 + M(\alpha)x(S(\alpha) - T(\alpha))$$

17 
$$Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$$

18 to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the elliptic  
19 curve  $E$ .

1 29. (Currently Amended) The storage medium of Claim 26,  
2 wherein the acquiring step

3 (a) in the first case acquires affine coordinates

4 
$$(\cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)}) (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

5 
$$(\cancel{X2(\alpha)}, \cancel{\beta x Y2(\alpha)}) (\phi_2(\alpha), \beta x \phi_2(\alpha))$$

6 of the two different points on the elliptic curve  $E$  and the operation information  
7 indicating the addition, and

8 (b) in the second case acquires affine coordinates

9 
$$(\cancel{X1(\alpha)}, \cancel{\beta x Y1(\alpha)}) (\phi_1(\alpha), \beta x \phi_1(\alpha))$$

10 of the single point on the elliptic curve  $E$  and the operation information indicating  
11 the doubling,

12 wherein the transforming step

13 (a) in the first case performs the coordinate transformation on the acquired  
14 affine coordinates of the two different points to generate Jacobian coordinates

15 
$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

16 
$$(X2(\alpha) : Y2(\alpha) : \beta x Z2(\alpha))$$

17 of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta x Z1(\alpha))$$

of the single point, and

wherein the operating step

(a) in the first case computes

$$U1(\alpha) = X1(\alpha) \times Z2(\alpha) \{ 2$$

$$U2(\alpha) = X2(\alpha) \times Z1(\alpha) \{ 2$$

$$S1(\alpha) = Y1(\alpha) \times Z2(\alpha) \{ 3$$

$$S2(\alpha) = Y2(\alpha) \times Z1(\alpha) \{ 3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha) \{ 3 - 2 \times U1(\alpha) \times H(\alpha) \{ 2 + r(\alpha) \{ 2$$

$$Y3(\alpha) = -S1(\alpha) \times H(\alpha) \{ 3 + r(\alpha) \times (U1(\alpha) \times H(\alpha) \{ 2 - X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

to obtain Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the elliptic curve  $E$ , and

(b) in the second case computes

$$S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha) \{ 2$$

$$M(\alpha) = 3 \times X1(\alpha) \{ 2 + a \times Z1(\alpha) \{ 4 \times f(\alpha) \{ 2$$

$$T(\alpha) = -2 \times S(\alpha) + M(\alpha) \{ 2$$

40 and computes

41 
$$X3(\alpha) = T(\alpha)$$

42 
$$Y3(\alpha) = -8xY1(\alpha) \{ 4 + M(\alpha) x(S(\alpha) - T(\alpha))$$

43 
$$Z3(\alpha) = 2xY1(\alpha)xZ1(\alpha)$$

44 to obtain the Jacobian coordinates  $(X3(\alpha) : Y3(\alpha) : \beta x Z3(\alpha))$  of the point on the

45 elliptic curve  $E$ .

1 30-33. (Cancelled)